200a, 200b, are integrated into the same fibre 10. Thus, it is respectfully submitted that the sensing system is both the laser 100a which produces the light which is used in the sensing technique, as well as the detector and processor which detect that light and process signals to determine an alarm condition.

In response to the Examiner's objection to claim 13 in section 5, Applicants have replaced "suppled" in claim 13 with "supplied."

In response to the Examiner's objections to claims 16-18 in section 6, Applicants have amended claims 16-18 to depend from claim 15.

Accordingly, Applicants respectfully request the Examiner to withdraw the objections to the specification and the claims.

With reference to section 7 and the rejection based on US Patent 5,455,698 to Udd, we respectfully submit that the claims are clearly patentable over this reference. The reference is not concerned with the essence of the present invention and in no way teaches or suggests the subject matter of claim 1 or any of the other claims in this application.

The present invention is concerned with actually locating the position of a disturbance to a structure. The structure will generally be a building, pipeline or the like. However, the structure could well be a communication link, as is shown in the embodiment of Figure 4. Regardless of the nature of the structure, the essence of the present invention is actually to locate the position of the disturbance so the position can be readily identified. In order to do this, the present invention provides a light source and a waveguide for receiving light from the light source so the light is caused to propagate in both directions along the waveguide to thereby provide counter-propagating optical signals in the waveguide. The waveguide being capable having the counter-propagating optical signals, or some characteristic of the signals modified or effected by an external parameter caused by or indicative of the event to provide modified counter-propagating optical signals. The invention further includes a detector for detecting the modified counter-propagating signals effected by the parameter and for determining the time delay between the modified counter-propagating optical signals, so that the location of the event can be determined.

As is made clear in the specification, if the difference in time of arrival of each of the modified counter-propagating signals is detected, then the point along the fibre at which the event or disturbance occurred can be calculated by the equations which are set out on page 20 of the specification. This therefore enables the exact position of the disturbance or event to be determined so that appropriate remedial action can be taken, such as, inspection of the sight of the disturbance for repairs, and for security checks.

US Patent 5,455,698 to Udd is not concerned with determining the actual location of a disturbance or an event. Rather, Udd specifically relates to communication networks and is concerned with preventing data from being tapped off and used by an intruder.

This is a significant difference between the present invention and Udd because, in the present invention, the system does not protect the data other than to identify the position of an intrusion if the system is actually used with a communication link. In Udd, the purpose of the system is to protect the data so that if someone does attempt to tap off data, that data cannot be identified by the intruder, but does not locate the actual position of that tap off.

As is explained in Udd at column 1, line 61 to column 2, line 45, Udd is based on a combination of information or data being impressed on the relative phase difference between counter-propagating light beams and the low coherence length of the light source used to create those beams. Because the information in Udd is impressed between two counter-propagating light beams, the two beams must be mixed to extract the signal. Since recorders do not exist at the frequencies referred to in Udd, this must be done in real time. An intruder trying to tap the system would first have to access both counter-propagating beams if the system were to be passively tapped. In addition, the intruder would have to access both counter-propagating beams and match the path length of the two beams to within a few coherence lengths characteristic of the light source in order that the amplitude modulated output signal may be constructed. Since the counter-propagating path lengths may differ by kilometers at the point of interception, and since the coherence length of a low coherence light source such as a light emitting or super-radiant diode may be in the order of 30 microns, tapping into the system becomes an extremely difficult and time-consuming task.

Udd actually compares this to attempting to find a needle in a haystack, which is an extremely good analogy consistent with the view that Udd is attempting to protect the data if tapped off rather than locating the position at which the data is actually being tapped.

Udd further explains, to make the system even more secure, a random path length generator may be used to randomly vary the relative path length of the two counter-propagating beams. Udd also explains that this is equivalent to having the needle in a haystack move randomly throughout the haystack. In the unlikely event the intruder manages to achieve the path length matching condition, a new equally difficult path length condition chosen totally at random, occurs a short time later. Udd again explains that this is analogous to luckily stumbling on the needle in the haystack, only to have it hidden once again at some random location in the haystack at an instance later.

Udd still further explains that an alternative approach is to utilize optical power alarm systems that preclude the potential intruder from obtaining information even if path length matching conditions should occur. Again, Udd explains that this is analogous to making the needle in the haystack dim and disappear.

The basic nature of the system provided by Udd is best described with reference to Figure 1.

Figure 1 shows a system in which a Sagnac interferometer communication link 101 is provided. The system has a receiver 103 and a transmitter 105. The receiver 103 includes a light source 111 and a detector 117. Depolarising elements 113 are used to depolarise the light signal, or alternatively, polarisation preserving fibres could be used, but this would greatly increase costs. The light source 111 is connected to a beam splitter 115 which causes light to be launched into two fibres 107 and 109 so as to propagate in opposite directions with respect to one another.

The transmitter 105 includes a phase modulator 119 which impresses phase information upon the light beam propagating in the two opposed directions, so that when the beams recombine and interfere, an amplitude modulated light signal is provided which is detected by the detector 117.

Thus, the purpose of the counter-propagating signals in Udd is to enable the impression of phase information upon each of the two signals which then propagate in opposite directions, and when recombined, interfere to produce a modulated signal which actually carries the data which is to be detected.

This is completely different to the present invention as claimed in claim 1. In claim 1 of the present application, the two counter-propagating signals are produced so as to run in counter-propagating or opposite directions with respect to one another so that an event at the waveguide, such as an attempt to tap into the waveguide or other disturbance to the waveguide, causes the counter-propagating signals to change in character to thereby produce modified counter-propagating signals which effectively then propagate onwardly from the location of the disturbance.

In the present invention, the detector detects the modified counter-propagating signals and determines the time delay between the modified counter-propagating signals so that the location of the event can be determined in the manner which we have described above. We stress that this is completely different to the purpose of the counter-propagating signals in Udd, which is to actually carry the data signal by impressing phase data onto each of the counter-propagating signals, so that when they recombine and interfere, a modulated signal carrying the data is produced for detection.

Since Udd uses the counter-propagating techniques to actually carry the data and to ensure that even if the fibre is tapped, the data cannot be extracted, it is necessary that the light source used by Udd be a short coherence length light source. The present invention does not require such a source because of the inherent difference between the purpose of the counter-propagating signals in the present invention and those in Udd.

Referring now to Figure 8, which is the figure the Examiner seems to primarily rely upon in his rejection of claim 1, we comment as follows.

Figure 8 illustrates what occurs in Udd when there is a tap of the system. As is explained in Udd, it is assumed that the tapper locates a fibre having portions 805 and 807 which are tapped to the system by a beam splitter 801. The portions 805 and 807 are also connected to a beam splitter 809, which has one arm connected to a detector 811. Thus, this enables signals propagating in both directions to be tapped off the fibre loop 803 of Udd which carries the communication signals and to be supplied to the detector 811.

This embodiment of Udd uses an additional element, namely path length generator 813 which is located along the fibre loop 803.

This embodiment has a light source 819 and a detector 823 which are the same as the light source 111 and detector 117 described with reference to Figure 1. The embodiment also includes the polarising elements 820 which are the same as the elements 113 in Figure 1.

Udd explains in relation to this embodiment that once the intruder has tapped into the fibre loop 803 and coupled the counter-propagating light beams into his device (i.e. loop 805, 807), the counter-propagating light beams tapped off would then have to be path length matched to high accuracy before the signal could be extracted. At lines 9 to 20 of column 8 of Udd, it is explained that a conventional light-emitting diode has a coherence length of about 35 microns.

For a multi-kilometer system, the intruder would be faced with the prospect of matching kilometer lengths to the order of 30 to 40 microns. In the system shown in Figure 8, the length of the fibre length 805 should be matched to the distance La and the fibre length 807 should be matched to the distance Lb before the beams are combined on the intruder's beam splitter 809 if the beams are to interfere to cause an amplitude modulated signal to result on the detector 811. Matching kilometer lengths of fibres to distances on the order of 100 microns is an extremely difficult and time consuming task. Udd again uses the analogy of looking for a needle in a haystack, and explains that in many cases, even the simplest system without the random path length generator 813, may provide sufficient security. By the additional inclusion of the path length generator 813, the path length can be randomly altered at very short time intervals, making it virtually impossible to get the path length match which is required in order to produce the interference and therefore the modulated signal which carries the data.

Referring to paragraph 9 of the official action, the Examiner equates the loop 803 with the waveguide defined in claim 1. Whilst the loop 803 is obviously a waveguide, there is no disclosure of the waveguide being capable of having counter-propagating optical signals modified or effected by an external parameter to provide modified counter-propagating optical signals which continue to propagate along the waveguide. The Examiner also equates the item 823 to the requirement in claim 1 of the detector… which determines the location of the event. More importantly than the issue of the waveguide referred to in the previous paragraph, Udd simply does not define the detector which performs this function or is capable of performing this function. The item 823 in Udd is the detector which detects the recombined signal so that the data can be extracted. It is the same detector as the detector 117 which is included in Figure 1, as has been mentioned above. The description of Figure 8 says nothing about the detector 823, other than light returned to the beam splitter 821 is in turn connected back to the detector 823. Nothing more is mentioned and, quite clearly, the detector is the same as detector 117 which extracts the communication signal which is provided by the impression of the phase information by the transmitter 825.

There is no disclosure or suggestion in Udd that the detector be for detecting the modified counter-propagating signals effected by the parameter and which are created when the fibre is disturbed and which determine the <u>time difference</u> between the receipt of the modified counter-propagating signals in order to <u>determine the location</u> of the event.

Udd is completely silent to determining the location of the event, and as has been explained in detail above, is not the slightest bit concerned with this. Udd is concerned with preventing the information from being able to be "recognised" if an attempt is made to tap off from the loop 803 by means of a tap such as that shown by items 801, 805, 807, 809 and 811 in Figure 8.

Thus, there is no suggestion or teaching in Udd of the counter-propagating signals being modified in the waveguide by an event such as a disturbance to produce counter-propagating modified signals, and then a detector for detecting the modified signals to determine the time difference between the receipt of the signals to determine the location of the event.

Similar comments apply to all of the other embodiments disclosed in Udd, and none of those embodiments suggest or teach the features of claim 1 which have been discussed above. Thus, the claims are clearly novel and inventive over the other embodiments in Udd. In particular, we mention that in the embodiment of Figure 10 of Udd, a technique is used to determine an intrusion by tapping off signals to output detectors 1023 and 1025 which are connected to ratio transducer 1031. The ratio transducer 1031 produces a ratio of the strength of the signals tapped off so that if there is a change, an intrusion is identified. However, once again, this merely identifies the fact that an intrusion has taken place and does not locate the intrusion. There is no suggestion of detecting modified counter-propagating signals and determining the time difference between receipt of those signals so that the location can be determined.

A still further modification in Udd suggests not only detecting the signal strength as in Figure 10, but also detecting spectral components so that the entire bandwidth of interest can be monitored. Once again, signals are supplied to a ratio alarm system where a ratio at various frequencies is determined. Once again, this system merely alerts to the fact that an intrusion has taken place, but does not locate the intrusion as required by the present invention.

Since claim 1 is clearly novel and inventive over the disclosure in Udd, we respectfully submit that all of the claims dependent on claim 1 are also novel and inventive.

In relation to claim 6 and paragraph 13 of the official action, we respectfully submit that Udd also does not suggest the further features recited in this claim. The items referred to by the Examiner, with respect, are not additional waveguides to introduce additional time delay, and there is no suggestion or teaching of this in Udd.

In relation to paragraph 14, the two detectors referred to in Udd and numbered 2325 and

2327 and the processing means do not determine the time delay or difference between the signals effected by the disturbance. There is no suggestion or disclosure of the determination of any time delay in Udd and, as explained above, Udd simply does not do this. As is specified clearly at lines 3 to 20 of paragraph 18 of Udd, the taps 2321 and 2323 are used to monitor the output from the light source. The ratio of light power on detectors 2327 and 2331 can be used to normalize any deviations from the stable split of the optical power, and the sum of the power on the detectors monitors the total light injected. The detectors can be used for direct detection of power level and their ratio can be used to detect an attempt to make unauthorized signal side taps. There is no suggestion of determining time differences or locating the actual location of a disturbance or event.

Similar comments apply to method claim 15 as apply to claim 1. Again, there is no suggestion in Udd of producing modified counter-propagating optical signals upon an intrusion into the waveguide and detecting the modified counter-propagating signals to determine the time difference between the receipt of the signals to determine the location of the event. Column 18, lines 6 to 10, which is referred to by the Examiner at the end of paragraph 22, has been discussed above and does not suggest the determine of any time differences or the use of those time differences to actually locate the event. Indeed, all that the lines referred to by the Examiner state is that the taps are used to monitor the output from the light source, the performance of the beam splitter and the light power of the counter-propagating light beams generated by the light source. There is absolutely no suggestion or teaching of determining the time difference and locating the event. As has been explained above in great detail, Udd is simply not concerned with this and does not remotely suggest this, let alone disclose this essential aspect of the present invention.

Similar comments apply to claim 19. Once again, this claim clearly defines the concept of producing the modified counter-propagating signals and detecting the modified counter-propagating signals so the time difference between the receipt of the signals is measured and utilized to determine the location of the sensed event. Since Udd does not disclose these features, this claim is also clearly novel and inventive over Udd.

Claim 20 is specifically concerned with the inventive concept applied to a communication link. Again, there is no suggestion in Udd of producing the counter-propagating optical signals which have the modified characteristic and detecting the modified counter-propagating signals so the time difference between the receipt of the signals is determined in order to determine the location of the disturbance.

Claim 26 is a method claim which corresponds to claim 20, and this claim also is considered patentable over Udd for the same reasons as expressed in relation to all of the other claims mentioned above.

We therefore respectfully submit that the claims are clearly not taught or remotely suggested by Udd, and therefore all of the claims are clearly patentable over Udd.

With reference to section 33 of the report, we confirm that the subject of all the claims was commonly owned. As to section 34, since claims 1 and 20 are patentable over Udd, claims 2 and 21 which are dependent on those claims are also patentable over Udd.

The Examiner is invited to contact the undersigned attorney should the Examiner determine that such action would facilitate the prosecution and allowance of the present application.

Respectfully submitted,

Glen A. Weitzer
Reg. No. 48,337

Docket No.: 43153-9062-00
Michael Best & Friedrich LLP
100 East Wisconsin Avenue
Milwaukee, Wisconsin 53202-4108

(414) 271-6560

APPENDIX

13. (Amended) The method of claim 11 wherein data signals are [suppled] supplied to the waveguide so that the waveguide acts as a communication link for transmission of data from one place to another and the launching of the counter-propagating optical signals in the waveguide enables the integrity and security of the waveguide to be monitored.

16. (Amended) The method of claim 15 [13] wherein the light is launched into both ends of the waveguide to provide the counter-propagating signals.

17. (Amended) The method of claim 15 [13], wherein the light is launched into both ends of the waveguide from a single light source.

18. (Amended) The method of claim 15 [11], wherein the parameter is quantified and/or identified from the modified signals.